

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

FILED

MAR 28 2024

CLERK, U.S. DISTRICT COURT
NORFOLK, VA

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*One (1) laptop (Black MSI Notebook) and Toshiba Hard
Drive, located at the FBI, 509 Resource Row,
Chesapeake, VirginiaUNDER SEALCase No. 2:24sw 56

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. §§ 2252(a)(2)/(a)(4)


*Offense Description*Receipt/Possession of Child
Pornography

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA

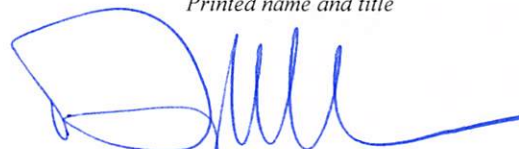

 Elizabeth M. Yusi, AUSA

Sworn to before me and signed in my presence.

Date: 03/28/2024City and state: Norfolk, VA

Applicant's signature

Kathryn J. Nguyen, Special Agent, FBI

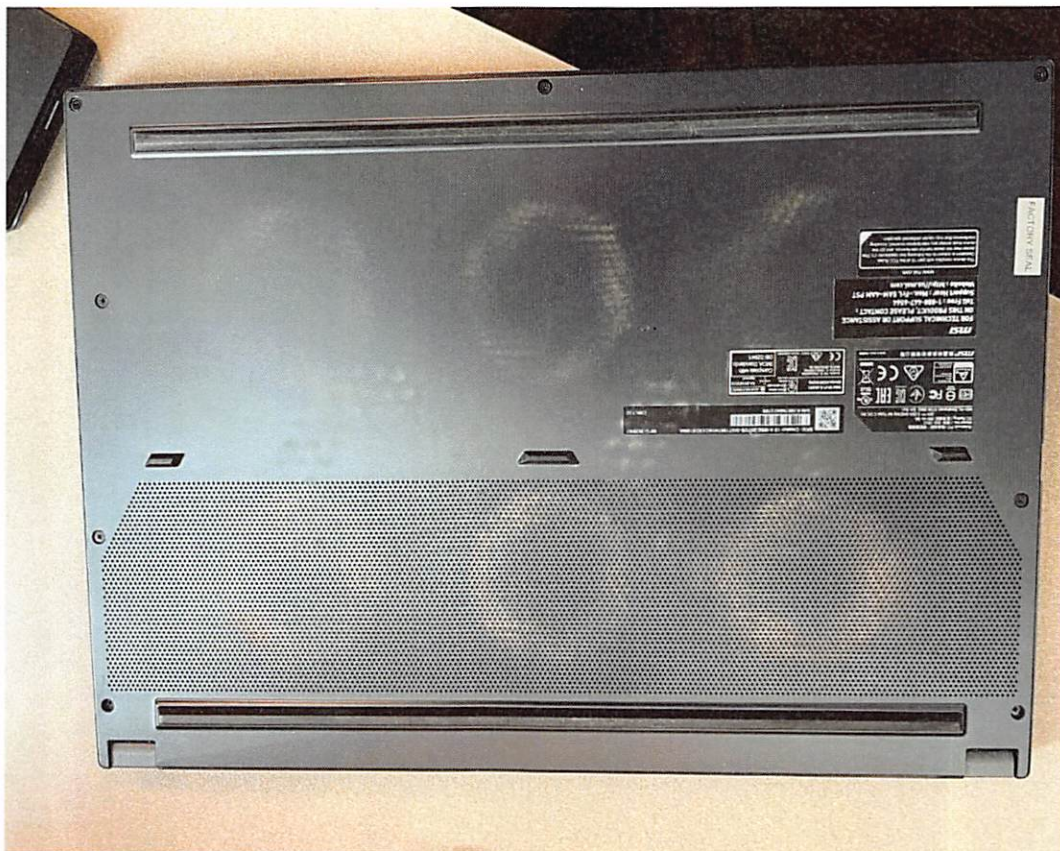
Printed name and title

Judge's signature

Douglas E. Miller, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

The property to be searched is One (1) BLACK MSI NOTEBOOK PC LAPTOP and One (1) TOSHIBA EXTERNAL HARD DRIVE (hereinafter “SUBJECT DEVICES”) currently in the possession of the Federal Bureau of Investigation, 509 Resource Way, Chesapeake, Virginia.





2.

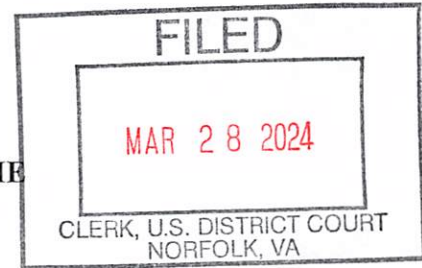
ATTACHMENT B
Items to be Searched For, Seized, and Examined

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252(a)(2) – Receipt of Child Pornography, and 18 U.S.C. § 2252(a)(4)(B) – Possession of or Accessing with Intent to View Child Pornography, collectively referred to as the “Target Offenses,” including:

1. All records, documents, or materials, including correspondence, that pertain to the identification of the users of electronic media during the relevant time period;
2. Any records, documents, or materials, including encryption codes, encryption links, or passcodes related to the online storage or cloud-based accounts;
3. Any records, documents, or materials, including any correspondence, that involve any communication with any person concerning the sexual exploitation of a minor;
4. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
5. All originals and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
6. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
7. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
8. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
9. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs;
10. Any records, documents, or materials referring or pertaining to communication with others, whether in person, by telephone, or online, for the purpose of distributing or transporting child pornography, including chat logs, call logs, address book or contact list entries, and digital images or videos sent or received; and

11. Information or evidence of any websites visited, photographs, videos, images, reports, definitions, stories, books, music, lyrics, emails, videos, messages, and or notes associated with child pornography or those who collect, disseminate, or trade in child pornography.

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF:

One (1) LAPTOP (Black MSI Notebook PC
with SN K2007N0072750) and One (1)
Toshiba Hard Drive, LOCATED AT THE
FBI, 509 RESOURCE ROW,
CHESAPEAKE, VA

Case No. 2:24-SW

SG

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH**

Your affiant, Kathryn J. Nguyen, being first duly sworn, hereby deposes and states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant and make arrests.

2. I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (FBI). I have been employed by the FBI as a Special Agent since September 2015. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, § 2510(7). That is, I am an officer of the United States, who is empowered by law to conduct investigations regarding violations of United States law, to execute warrants issued under the authority of the United States, and to make arrests of the offenses enumerated in Title 18, United States Code. In the course of my duties, I am responsible for investigating crimes which include, but are not limited to, child exploitation and child pornography. I have previously been involved in criminal investigations concerning violations of

federal laws. Since joining the FBI, your affiant has received specialized training in child exploitation investigations, identifying and seizing electronic evidence, computer forensics, recovery of electronic files, electronic device imaging, and social media website investigations.

3. Your affiant makes this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a laptop device and external hard drive described in Attachment A (the “SUBJECT DEVICES”) – and the extraction from that property of electronically stored information described in Attachment B.

4. This affidavit is based upon information that I have gained from my investigation, my training and experience, as well as information provided my personal knowledge, and that of other sworn law enforcement officers participating in this investigation including the United States Marshals Service (USMS). Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of violations of 18 U.S.C. § 2252(a)(2) (receipt of child pornography) and 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) are located on the SUBJECT DEVICES.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched, the SUBJECT DEVICES, are a black MSI Notebook PC Laptop and Toshiba hard drive (described more fully in Attachment A and incorporated) which, as discussed below, was sent by the finder, B.S. to Deputy United States Marshal (DUSM) Jeffrey Imgrund of the USMS after [↑]ROSS's arrest in Pe Ell, Washington. The

SUBJECT DEVICES were provided by DUSM Imgrund, to FBI Norfolk, 509 Resource Row, Chesapeake, VA 23320, where it was submitted to evidence, for the purpose of analyzing the computer pursuant to a search warrant issued by this Court (*see* 2:24sw33), as detailed below.

6. The applied-for warrant would authorize the seizure and forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B (incorporated herein by reference) for violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B).

SPECIFIED FEDERAL OFFENSES

7. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and such visual depiction is of such conduct;

8. 18 U.S.C. § 2252(a)(4)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or

affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped, or transported, by any means including by computer.

DEFINITIONS

9. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

10. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

11. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device,” and includes smartphones, mobile phones, and devices. See 18 U.S.C. § 1030(e)(1).

12. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and

related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

13. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

14. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

15. “Internet Protocol Address” (IP Address), as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

16. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

17. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

18. DENNIS ROSS pleaded guilty to Receipt of Child Pornography, in violation of 18 U.S.C. § 2252(a)(2), 2256(1), and 2256(2), on May 27, 2010, in this Court. *United States v. Ross*, 2:10cr84 (E.D.Va. (Norfolk) 2010) (M. Davis). On September 3, 2010, he was sentenced to 60 months’ imprisonment, supervised release for 25 years, and a \$10,000 fine. He was released from the Bureau of Prisons on or about October 3, 2014.

19. ROSS was subsequently classified as a Tier 1 sex offender pursuant to Virginia State Code, which required him to register as a sex offender for the duration of his life every 90 days.

20. In October 2014, ROSS signed a Virginia Sex Offender Registration form while in the custody of the Virginia State Police. On that form, ROSS provided a physical home street address in Suffolk, Virginia. The form also included a notice, signed by ROSS, informing him that he will be responsible to regularly re-register and provide, among other things, his physical address on at least on an annual basis.

21. ROSS was subsequently found to be in violation of his supervised release conditions on or about August 23, 2018. On November 19, 2018, ROSS had a supervised release

violation hearing in front of Judge M. Davis. The court withheld finding on the violation and continued the hearing until May 23, 2019. On or about May 21, 2019, Judge M. Davis dismissed the violation petition prior to the May 23, 2019, hearing.

22. On October 13, 2022, a warrant was issued and delivered to USMS for ROSS for various violations of his supervised release. On October 4, 2022, the U.S. Probation Office attempted a home visit with ROSS at his given address at a hotel and he was not there. The hotel stated he left months earlier. ROSS failed to update his sex offender registration within three (3) business days, as required by the SORNA and absconded from supervision of the U.S. Probation Office.

23. On November 1, 2022, Virginia State Police entered an arrest warrant into the National Criminal Information Center (NCIC) with charges to failure to register as a sex offender. In addition, this Court issued an arrest warrant for ROSS due to his violations of his supervised release conditions.

24. In or about November or December 2023, Lewis County Sheriff Department learned that ROSS was living in Pe Ell, Washington. On December 12, 2023, ROSS was arrested in the Western District of Washington. The arrest took place on the property belonging to B.S. ROSS was extradited to the Eastern District of Virginia on the warrant issued for a supervised release violation petition.

25. On February 5, 2024, the USMS contacted B.S. to follow up about a few specifics regarding the investigation into ROSS. B.S. informed the USMS of a laptop and hard drive (the SUBJECT DEVICES) belonging to ROSS being at her residence that was left behind after his arrest. B.S. observed the laptop in ROSS' possession constantly. ROSS played "games" online. ROSS was on the laptop at the time of his arrest.

26. In February 2024, B.S. provided the SUBJECT DEVICES to the USMS in Norfolk, VA, via mail. USMS applied for and this Court issued a search warrant for the computer to search for evidence concerning his failure to register as a sex offender. *See* 2:24sw33.

27. Both the laptop and external hard drive (the SUBJECT DEVICES) were provided to the FBI Norfolk field office for a forensic review, where they were submitted into evidence.

28. During a forensic review of the laptop's media by the FBI's Computer Analysis Response Team (CART), images of child sexual abuse material (CSAM) were observed in plain view. As an example, one specific image depicted a prepubescent female child laying naked on a bed. The prepubescent female child's legs were spread, exposing her vagina, and her hand was resting by the top of her vagina.

CONCLUSION

29. Based on the aforementioned factual information, I respectfully submit that probable cause exists to believe that a user of the SUBJECT DEVICES received and possessed child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which prohibit the knowing receipt and possession of visual depictions of and involving the use of a minor engaging in sexually explicit conduct.

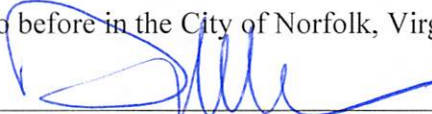
30. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities of such violations will be found on the SUBJECT DEVICES belonging to ROSS. Accordingly, I request that a warrant be issued authorizing me, with assistance from additional FBI personnel, to search the SUBJECT DEVICES for evidence, fruits, and instrumentalities of these offenses.

Respectfully submitted,



Kathryn J. Nguyen, Special Agent
Federal Bureau of Investigation

Sworn to before in the City of Norfolk, Virginia, on March 28, 2024



UNITED STATES MAGISTRATE JUDGE

Douglas E. Miller
United States Magistrate Judge